UPPSALA UNIVERSITET

Cybersecurity in Industrial Control Systems

André M.H. Teixeira

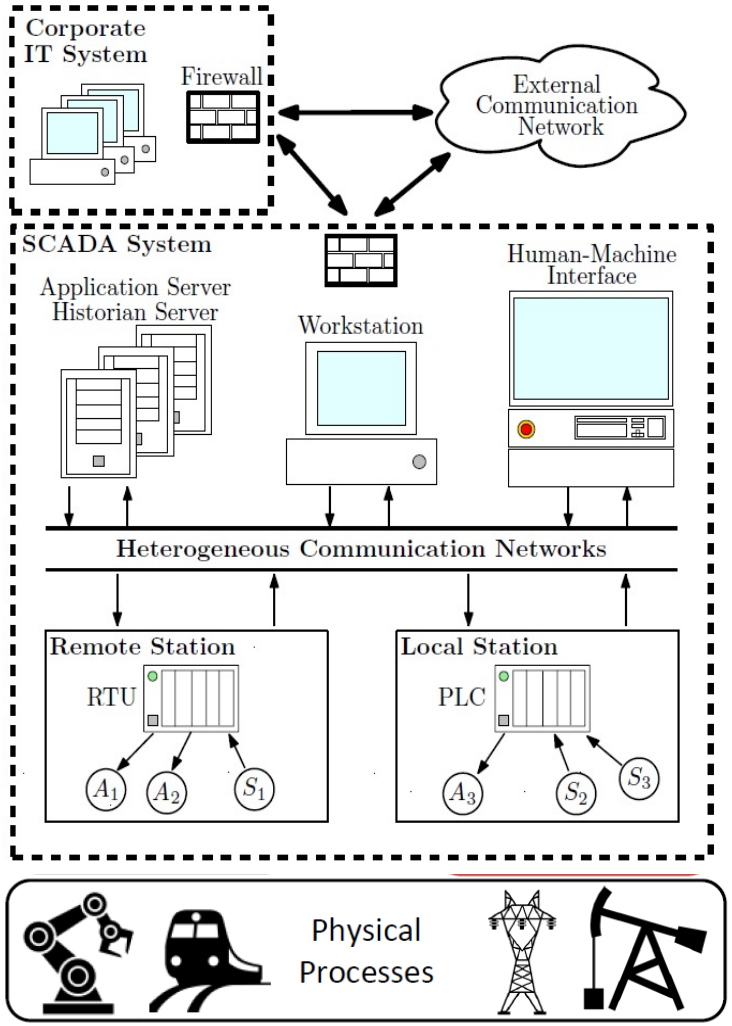
Dept. Electrical Engineering
Uppsala University

Riskförmiddag i Uppsala
3 December 2020

UPPSALA UNIVERSITET

Typical Vulnerabilities in Industrial Control Systems

- Computers in control center do not have adequate protection
  - No anti-virus or intrusion detection, USB-ports accessible
- Communication links lack basic security features
  - No encryption or authentication
- Lack of physical protection
  - PLCs and RTUs accessible
- Zero-day vulnerabilities



Example: Stuxnet (2010)

- **Targets:** Windows, ICS, and PLCs connected to variable-frequency drives
- Exploited **4 zero-day vulnerabilities**

- **Speculated goal:**

Harm centrifuges at uranium enrichment facility in Iran

- **Attack mode:**

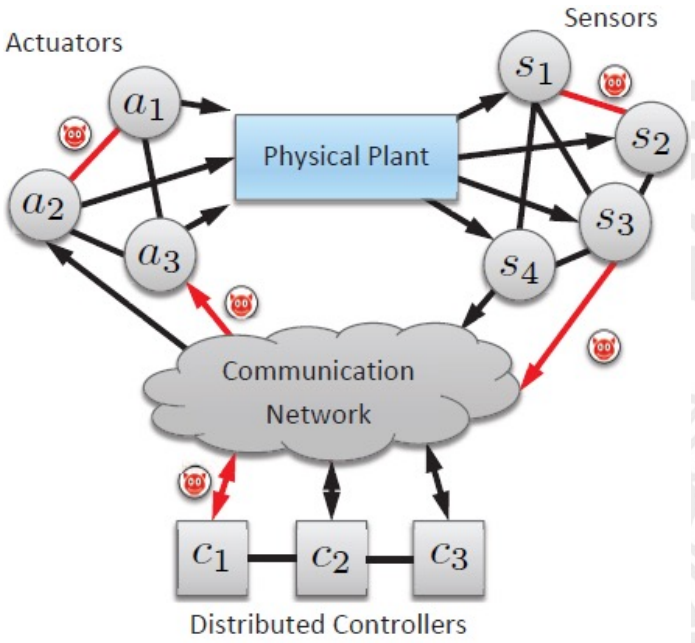
1. Delivery with USB stick (**no internet connection necessary**)
2. Replay measurements to control center and execute harmful controls

["The Real Story of Stuxnet", IEEE Spectrum, 2013]

Cyber-Secure Control Systems

Modern Industrial Control Systems

- are being **integrated with business/corporate networks**
- have many potential points of **cyber-physical attack**

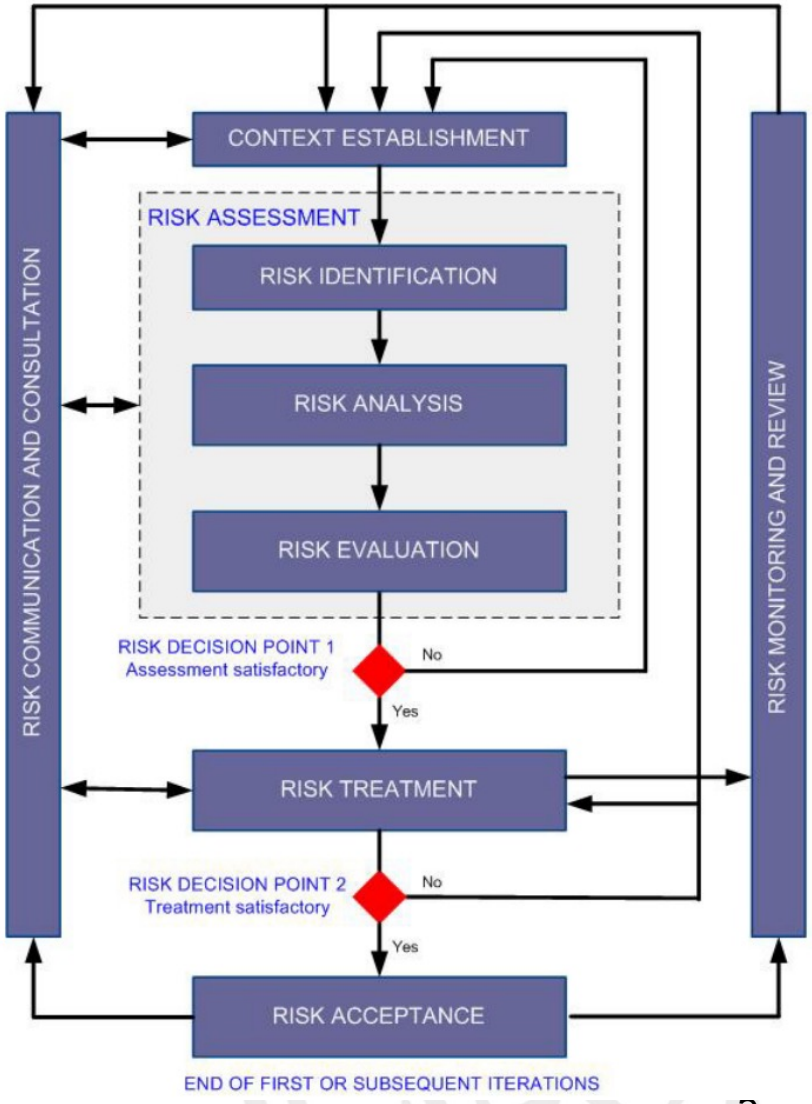


Need tools and strategies to understand and mitigate attacks:

- **Which threats** should we care about?
- **What impact** can we expect from attacks?
- **Which resources** should we **protect** (more), and how?
- **Answer: Risk management**

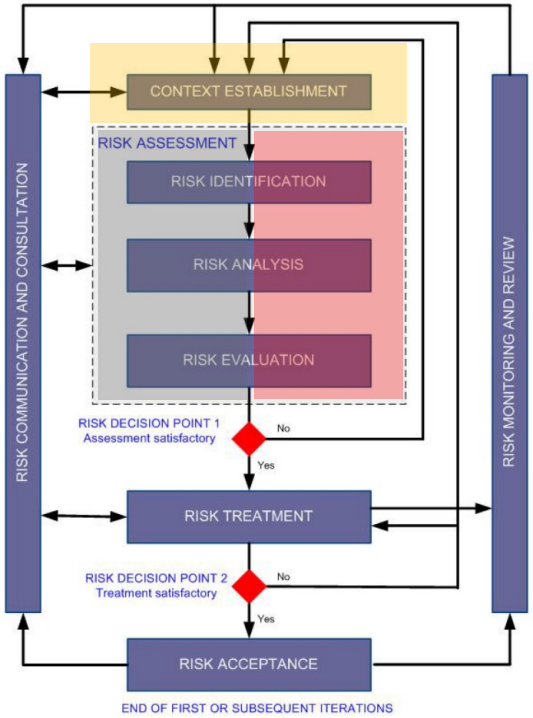
Cyber Risk Management

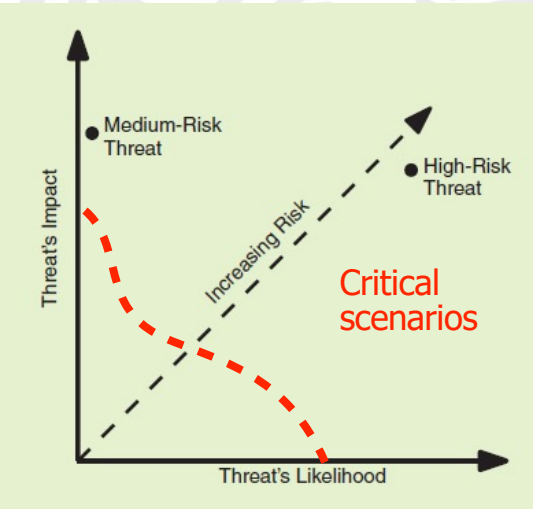
- Related Standards
  - ISO 27000 - Information security
  - ISO 31000 – Risk Management
- Conceptually similar to *Safety* Risk Management
- Similar tools can (often) be used
  - Attack Graphs (vs Fault trees)
  - Bayesian networks
- Different main focus:
  - Information system assets
  - Malicious adversaries



The Concept of Risk

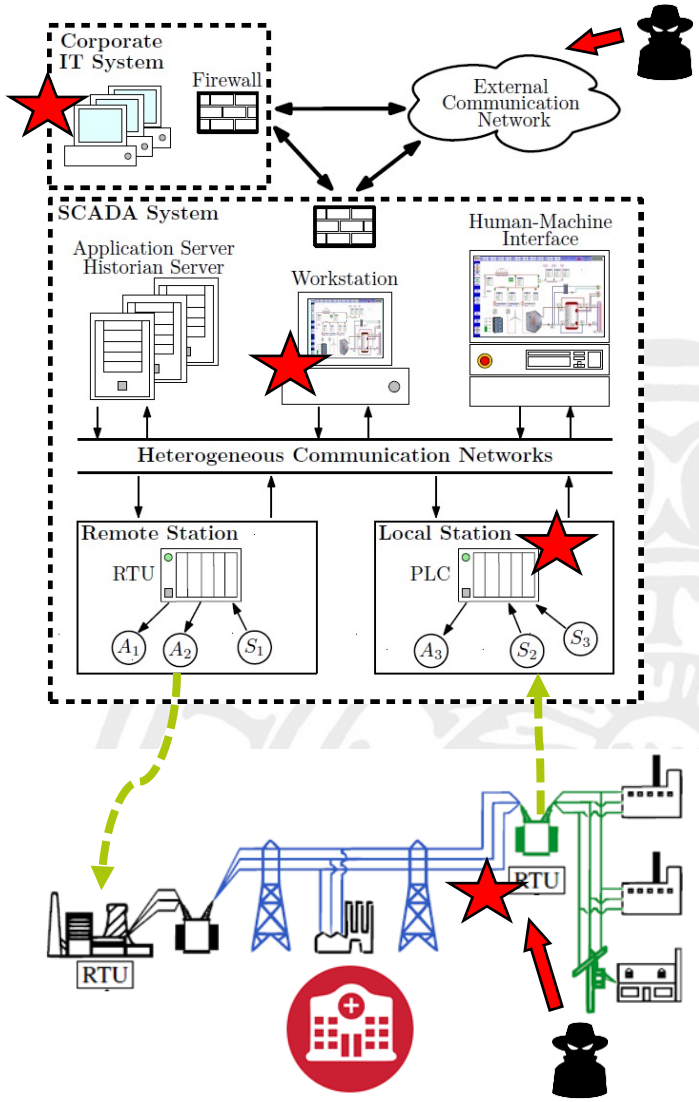
- [Kaplan & Garrick, 1981] Risk is a set of tuples:
  Risk = (Scenario, Likelihood, Impact)
  - Attack Scenario
    - What is the system?
    - What is the type of adversary?
  - Impact of the attack
    - What security properties were violated? What services were interrupted?
    - What are the consequences? (Financial, operational, reputation, human lives, …)
  - Likelihood of the attack
    - "Probability" of successful attack
    - Required capabilities, knowledge…





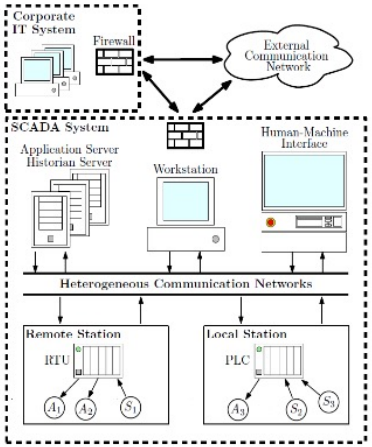
Likelihood Metrics for Industrial Control Systems

- Likelihood depends on ICT infrastructure
- Successful attack:
  - Successful initial infection
  - Sucessful dissemination of malware
  - Sucessful infection of target devices
  - Sucessful control of target devices
- Likelihood metric: probability of successful attack
  - Hard to compute – lack of historical data
  - Alternative: use proxy metrics that assess the attack effort, e.g.:
    - number of infected target devices
    - Required capabilities and knowledge
    - Number of vulnerabilities exploited
    - …



UPPSALA UNIVERSITET

Is More Than IT Security and Safety Needed?



- Clearly IT security and Safety are needed: Authentication, encryption, firewalls, redundancy, fault tolerance, etc.

But not sufficient…

- **Interaction between physical and cyber systems** make control systems different from normal IT systems
- **Malicious actions can enter anywhere** in the closed loop and cause harm, whether channels secured or not
- **Malicious attackers** have an **intent,** as opposed to faults, and can act strategically
- **Can we trust** the interfaces and channels are really secured? (see **OpenSSL** Heartbleed bug…)

- Security and Safety recommendations can contradict each other

UPPSALA UNIVERSITET

Final Thoughts

Security	=/=	Safety
Säkerhet	=/=	Säkerhet

Integration of safety and security:
necessary, but challenging!

Thank you!

andre.teixeira@angstrom.uu.se

Further Reading

- **Introduction to CPS/NCS security**
- Cardenas, S. Amin, and S. Sastry: “Research challenges for the security of control systems". Proceedings of the 3rd Conference on Hot topics in security, 2008, p. 6.
- Special Issue on CPS Security, IEEE Control Systems Magazine, February 2015
- D. Urbina *et al*.: ”Survey and New Directions for Physics-Based Attack Detection in Control Systems”, NIST Report 16-010, November, 2016
- **CPS attack models, impact, and risk management**
- A. Teixeira, I. Shames, H. Sandberg, K. H. Johansson: ”A Secure Control Framework for Resource-Limited Adversaries”. Automatica, 51, pp. 135-148, January 2015.
- A. Teixeira, K. C. Sou, H. Sandberg, K. H. Johansson: "Secure Control Systems: A Quantitative Risk Management Approach". IEEE Control Systems Magazine, 35:1, pp. 24-45, February 2015
- D. Urbina *et al*.: ”Limiting The Impact of Stealthy Attacks on Industrial Control Systems”, 23rd ACM Conference on Computer and Communications Security, October, 2016